

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-175403

(43)Date of publication of application : 02.07.1999

(51)Int.Cl.

G06F 12/14

G06F 12/16

G11C 16/02

G11C 29/00

(21)Application number : 09-335614

(71)Applicant : TOKYO ELECTRON LTD

(22)Date of filing : 05.12.1997

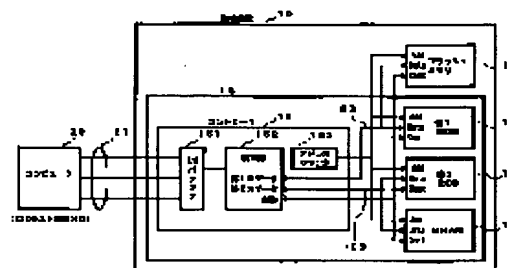
(72)Inventor : NAKAMURA YASUHIRO

(54) TEST METHOD FOR STORAGE DEVICE AND MEMORY PROVIDED WITH TEST FUNCTION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a test method for testing a storage area storing a decoding program without leaking an enciphered cryptographic key to the outside in a storage device for enciphering and storing data.

SOLUTION: An enciphered cryptographic key (k) is stored in a flash memory 11. A decoding program for decoding the cryptographic key (k) is stored in a ROM 14 where the access from the outside is inhibited and protected. The cryptographic key(k) is decoded by the decoding program, data are enciphered by using the cryptographic key (k) to store the data in the flash memory 11 and the data read from the flash memory 11 are decoded by the cryptographic key (k) to be outputted. The data constituting the decoding program are processed by a hash function stored in the ROM 14 for checking an area for storing the decoding program, the processed result is compared with an expected value and when they are coincident, it is judged that the storage area is normal.



LEGAL STATUS

[Date of request for examination]

03.10.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-175403

(43) 公開日 平成11年(1999) 7 月 2 日

(51) Int.Cl.⁶
 G 0 6 F 12/14 3 2 0
 12/16 3 3 0
 G 1 1 C 16/02
 29/00 6 7 1

F I
 G 0 6 F 12/14 3 2 0 A
 12/16 3 3 0 A
 G 1 1 C 29/00 6 7 1 Z
 17/00 6 0 1 A

審査請求 未請求 請求項の数13 O L (全 11 頁)

(21) 出願番号 特願平9-335614

(22) 出願日 平成9年(1997)12月5日

(71) 出願人 000219967

東京エレクトロン株式会社

東京都港区赤坂5丁目3番6号

(72) 発明者 中村 泰弘

東京都府中市住吉町2丁目30番地の7 東

京エレクトロン株式会社府中事業所内

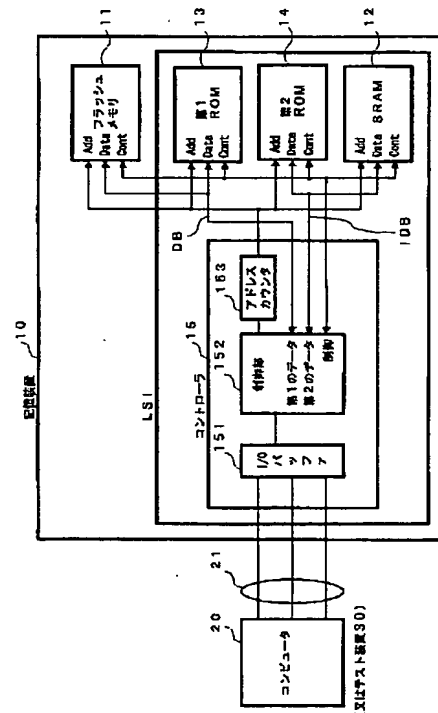
(74) 代理人 弁理士 木村 満 (外3名)

(54) 【発明の名称】 テスト機能を備える記憶装置及びメモリのテスト方法

(57) 【要約】

【課題】 データを暗号化して記憶する記憶装置において、暗号化された暗号鍵の復号プログラムを外部に漏らすことなく、かつ、復号プログラムを記憶エリアのテストを可能とするテスト方法を提供する。

【解決手段】 フラッシュメモリ11には、暗号化された暗号鍵kが記憶されている。外部からのアクセスが禁止されて、プロテクトされたROM14には、暗号鍵kを復号するための復号プログラムが記憶されている。この復号プログラムで暗号鍵kを復号し、この暗号鍵kを用いてデータを暗号化してフラッシュメモリ11に格納し、フラッシュメモリ11から読み出したデータを暗号鍵kで復号して出力する。復号プログラムを格納したエリアをチェックするため、復号プログラムを構成するデータをROM14に格納されたハッシュ関数で処理し、処理結果と期待値とを比較し、一致するとき、正常であると判別する。



【特許請求の範囲】

【請求項1】 データを記憶するための第1の記憶手段（フラッシュ11）と、暗号鍵が暗号化されて記憶されている第2の記憶手段（フラッシュ11）と、前記暗号鍵（k）を復号化するための復号情報が格納された第3の記憶手段（T2）と、前記第3の記憶手段をテストするための関数を記憶した第4の記憶手段（T4）と、前記第3の記憶手段に記憶された復号情報を用いて前記暗号鍵を復号化し、外部より供給されるデータを復号化した暗号化鍵を用いて暗号化して、前記第1の記憶手段に書き込む書込手段（15）と、前記第3の記憶手段に記憶された復号情報を用いて前記暗号鍵を復号化し、復号化された暗号鍵を用いて前記第1の記憶手段から読み出されたデータを復号化して出力する読出手段（15）と、前記第3の記憶手段に記憶された復号情報を前記第4の記憶手段に記憶された関数で処理し、得られた値と期待値を比較し、比較結果を出力する比較手段と（15）、を備えることを特徴とする記憶装置。

【請求項2】 前記第1、第2、及び第4の記憶手段の少なくとも1つの記憶手段のアドレスをスキャンして、その記憶内容を読み出すことにより、前記少なくとも1つの記憶手段の良否をテストするスキャン手段（152, 153）と、前記スキャン手段が、前記第3の記憶手段をアクセスすることを禁止する禁止手段（図7）と、をさらに備えることを特徴とする請求項1に記載の記憶装置。

【請求項3】 前記第1の記憶手段は、書き換え可能な不揮発性メモリから構成され、前記第2の記憶手段は、前記書き換え可能な不揮発性メモリの一部の領域から構成され、前記第3の記憶手段と前記第4の記憶手段は、不揮発性メモリから構成されている、ことを特徴とする請求項1又は2に記載の記憶装置。

【請求項4】 前記期待値は、この記憶装置に予め記憶されており、又は、外部から供給された値である、ことを特徴とする請求項1、2又は3に記載の記憶装置。

【請求項5】 前記関数は一方向性の関数（ハッシュ関数）である、ことを特徴とする請求項1乃至4のいずれか1項に記載の記憶装置。

【請求項6】 前記第3の記憶手段と前記比較手段は、一体に封止され（LSI）、前記第3の記憶手段と前記比較手段との通信内容は、外部に出力されないように構成されている、ことを特徴とする請求項1乃至5のいずれか1項に記載の記憶装置。

【請求項7】 機密情報を記憶する機密情報記憶手段（T2）と、

前記機密情報記憶手段をテストするためのテスト情報を記憶したテスト情報記憶手段（T4）と、外部より供給される前記機密情報記憶手段のテストを指示する指示信号を受信する受信手段（151）と、前記受信手段により受信された指示信号に応答し、前記テスト情報記憶手段に記憶されたテスト情報により前記機密情報を処理し、処理結果と期待値を比較し、比較結果を出力する出力手段（15, T3）と、を備えることを特徴とする記憶装置。

【請求項8】 前記テスト情報は、前記機密情報を処理する一方向性の関数（ハッシュ関数）から構成される、ことを特徴とする請求項7に記載の記憶装置。

【請求項9】 前記期待値は、この記憶装置に予め記憶されており、又は、外部から供給されて前記受信手段により受信された値である、ことを特徴とする請求項8に記載の記憶装置。

【請求項10】 前記機密情報は、データを暗号化及び／又は復号化するための暗号化された鍵を復号するための情報から構成され、

前記テスト情報は、所定の関数から構成される、ことを特徴とする請求項7、8又は9に記載の記憶装置。

【請求項11】 外部からの直接のアクセスが禁止されており、機密情報を記憶するメモリのテスト方法であって、

前記メモリに記憶されているデータを予め定められた方法で処理し、処理結果と期待値とを比較し、比較結果に基づいて、前記記憶内容の適否を判別する、ことを特徴とするテスト方法。

【請求項12】 外部からの直接のアクセスが禁止されており、暗号化された暗号化鍵を復号するための鍵復号情報を記憶するメモリのテスト方法であって、前記メモリに記憶されているデータを予め定められた方法で処理し、処理結果と期待値とを比較し、比較結果に基づいて、前記メモリに記憶された前記鍵復号情報の適否を判別する、ことを特徴とするテスト方法。

【請求項13】 前記予め定められた方法は、前記データを一方向性の関数で処理する方法である、ことを特徴とする請求項11又は12に記載のテスト方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、記録装置のテスト技術に関し、特に、暗号化鍵、暗号化鍵を復号するための情報、機密文書等の外部に対し秘密の状態に維持したい情報を記憶した記憶装置のテスト技術に関する。

【0002】

【従来の技術】 コンピュータ技術の発展に伴い、機密情報の保護の必要性が増大している。このため、データを暗号化して記憶したり、送信したりする暗号化技術の重要性が高まっており、コンピュータの外部メモリに格納するデータを暗号化して記憶すること等も実施されてい

る。例えば、記憶装置に暗号化鍵を格納しておき、記憶対象データをこの暗号化鍵を用いて暗号化してメモリに格納し、メモリから読み出されたデータを復号化鍵を用いて復号化することが行われている。

【0003】一方、製品の出荷時等に、記憶媒体の良否をチェックするためには、記憶媒体が正常にデータを記憶し、記憶したデータを出力できることを確認しなければならない。このため、従来は、予め定められたテストパターン等をメモリに記憶させてから、これを読み出して、両者を比較すること等が行われている。また、読み出し専用メモリについては、記憶データを読み出して、読み出したデータと書き込まれているデータとが一致するか否か等を確認している。

【0004】

【発明が解決しようとする課題】しかし、暗号化鍵を格納したメモリ装置を、この方法でテストすると、暗号化鍵自体が外部に読み出されてしまうという問題があった。

【0005】この問題を解決するため、メモリの記憶データを変換してから外部に読み出すようにしたテスト機能を備えるメモリ装置も提案されている。しかし、この方法でも、変形されたコードが外部に読み出されるため、変形の方法が推測され、暗号化鍵も推測できてしまうという問題があった。

【0006】また、特開平8-63402には、ROMに記憶されたデータと外部から供給する期待値とを比較して、比較結果を出力することにより、ROMの記憶データを直接外部に読み出すことなく、ROMをテストする機能を有する半導体集積回路が提案されている。しかし、この方法でも、アドレス単位等で、機密データが期待値に一致するか否かを知ることができるため、期待値を順次変更しながらテストすることにより、機密データを特定できてしまう。また、アドレス単位で比較動作を行うため、チェックに膨大な時間を要する。

【0007】この発明は上記実状に鑑みてなされたもので、データを暗号化して記憶する記憶装置において、暗号鍵等の機密性の高いデータを外部に漏らすことなく、かつ、メモリのテストを可能とするテスト方法及びテスト機能を備えた記憶装置を提供することを目的とする。また、この発明は、機密性の高いデータを格納した記憶装置のテストに適したテスト方法及びテスト機能を備えた記憶装置を提供することを目的とする。

【0008】

【課題を解決するための手段】上記目的を達成するため、この発明の第1の観点にかかる記録装置は、データを記憶するための第1の記憶手段（フラッシュ11）と、暗号鍵が暗号化されて記憶されている第2の記憶手段（フラッシュ11）と、前記暗号鍵（k）を復号化するための復号情報が格納された第3の記憶手段（T2）と、前記第3の記憶手段をテストするための関数を記憶

した第4の記憶手段（T4）と、前記第3の記憶手段に記憶された復号情報を用いて前記暗号鍵を復号化し、外部より供給されるデータを復号化した暗号化鍵を用いて暗号化して、前記第1の記憶手段に書き込む書込手段

（15）と、前記第3の記憶手段に記憶された復号情報を用いて前記暗号鍵を復号化し、復号化された暗号鍵を用いて前記第1の記憶手段から読み出されたデータを復号化して出力する読出手段（15）と、前記第3の記憶手段に記憶された復号情報を前記第4の記憶手段に記憶された関数で処理し、得られた値と期待値を比較し、比較結果を出力する比較手段と（15）、を備えることを特徴とする。

【0009】第3の記憶手段に復号情報が正しく記憶されているか否かをテストするため、第3の記憶手段の記憶データを外部から読めるように構成すると、復号情報が第三者に知られ、暗号化鍵を復号されてしまう虞がある。

【0010】そこで、この発明では、テスト用の関数を第4の記憶手段に記憶しておき、復号情報を関数で処理し、処理により得られた値と期待値を比較し、比較結果を出力する。復号情報が正しく記憶されていれば、一致を示す比較結果が出力されるはずであり、復号情報を外部に出力することなく、記憶されている1又は複数の暗号化鍵が正しいものであると判別することができる。また、復号情報を関数で処理し、その処理結果と期待値を比較しているため、期待値から復号情報を推測される虞もない。さらに、復号情報を関数で処理した値と期待値とを比較するので、アドレス単位で復号情報と期待値を比較する場合に比して、比較回数を減少させ、処理を高速化することが可能である。

【0011】第1、第2、第4の記憶手段については、その記憶内容をスキャンすること等により、正常であるか否かをテスト可能とし、第3の記憶手段については、スキャンアクセスを禁止する手段を配置してもよい。この構成においては、第3の記憶手段の記憶内容を直接アクセスして、その記憶データを読み出す行為も禁止され、復号情報の機密が保持される。

【0012】例えば、前記第1の記憶手段は、書き換え可能な不揮発性メモリから構成され、前記第2の記憶手段は、前記書き換え可能な不揮発性メモリの一部の領域から構成され、前記第3の記憶手段と前記第4の記憶手段は、不揮発性メモリから構成されている。この構成によれば、暗号化鍵を書き換え可能な不揮発性メモリに格納することができる。従って、記憶装置毎に暗号化鍵を異ならせ、一部の記憶装置の暗号化鍵が解読されても、他の記憶装置の暗号化鍵を推測できないように構成することも可能となる。

【0013】前記期待値は、この記憶装置の、例えば、上記不揮発性メモリに予め記憶されていてもよく、又は、外部から供給するようにしてもよい。

【0014】前記関数は、例えば、一方向性関数、例えば、ハッシュ関数である。復号情報を一方向性の関数により処理することにより、復号情報から処理結果の値は一義的に定まるが、処理結果から復号情報が多数予想され、復号情報を推測することが困難となる。

【0015】前記第3の記憶手段と前記比較手段は、樹脂等で一体に封止され、前記第3の記憶手段と前記比較手段との通信内容は、外部に出力されないように構成されることが望ましい。第3の記憶手段のデータライン等を他の記憶手段のデータラインと一体化すると、第3の記憶手段と比較手段との間でデータを授受している際にデータが外部に漏れる可能性がある。しかし、この構成によれば、第3の記憶手段の記憶内容を機密に保持できる。

【0016】また、この発明の第2の観点にかかる記憶装置は、機密情報を記憶する機密情報記憶手段(T2)と、前記機密情報記憶手段をテストするためのテスト情報を記憶したテスト情報記憶手段(T4)と、外部より供給される前記機密情報記憶手段のテストを指示する指示信号を受信する受信手段(151)と、前記受信手段により受信された指示信号に応答し、前記テスト情報記憶手段に記憶されたテスト情報により前記機密情報を処理し、処理結果と期待値を比較し、比較結果を出力する出力手段(15, T3)と、を備えることを特徴とする。

【0017】この発明においても、機密情報を外部に直接読み出すことなく、機密情報が正確に機密情報記憶手段に記憶されていることを判別できる。

【0018】前記期待値は、この記憶装置に予め記憶されている値でもよく、又は、外部から供給された値でもよい。

【0019】前記機密情報は、例えば、データを暗号化及び／又は復号化するための暗号化された鍵を復号するための情報から構成され、前記テスト情報は、例えば、所定の関数から構成される。

【0020】関数としては、例えば、ハッシュ関数等の多(関数に代入する値)対1(演算結果)の関係が成立する一方向性の関数が望ましい。なお、複数の機密情報、例えば、秘密鍵nと公開鍵eを機密情報記憶手段に記憶させても良い。この場合、例えば、 $m^e \bmod n = 0$ が成立するか否か等の比較結果から、機密情報が正しく記憶されているか否かを判別することができる。なお、mは外部から供給された又は内部に予め記憶されていた定数である。

【0021】また、この発明の第3の観点に関するテスト方法は、外部からの直接のアクセスが禁止されており、機密情報を記憶するメモリのテスト方法であって、前記メモリに記憶されているデータを予め定められた方法で処理し、処理結果と期待値とを比較し、比較結果に基づいて、前記記憶内容の適否を判別する、ことを特徴

とする。

【0022】これらのテスト方法によれば、メモリの記憶データを直接外部に読み出すことなくテストすることができる。しかも、処理後のデータを比較に使用するので、処理量を低減することも可能である。

【0023】前記機密情報は、例えば、暗号化された暗号化鍵を復号するための鍵復号情報、機密文書等である。

【0024】また、前記予め定められた方法は、例えば、前記データを一方向性の関数で処理する方法である。

【0025】

【発明の実施の形態】以下、この発明の実施の形態にかかるテスト機能を備える記憶装置を、フラッシュメモリを例に説明する。

【0026】図1は、この発明の第1の実施の形態にかかるテスト機能を備えるメモリ装置の構成を示す。図示するように、この記憶装置10は、フラッシュメモリ11と、SRAM12と、第1のROM13と、第2のROM14と、コントローラ15と、より構成される。

【0027】フラッシュメモリ11は、通常知られているように、ブロック消去型の記憶素子であり、複数のメモリセルから構成された複数のブロックを備え、予め消去されたブロックにのみデータの書き込みが可能なメモリである。フラッシュメモリ11には、データが暗号化されて記憶されている。このデータは、ファイルアロケーションテーブル(FAT)、ディレクトリ情報等のデータを含む。特定のアドレスT1には、データを暗号化及び復号化するためのデータ鍵kが暗号化されて記憶されている。

【0028】SRAM(スタティックランダムアクセスメモリ)12は、揮発性の高速メモリであり、フラッシュメモリ11に記憶されているデータの論理アドレスと該データが記憶されている位置の物理アドレスとの対応関係を記憶するアドレス変換テーブル、フラッシュメモリ11の書き込み可能なブロック(消去済みのブロック)の番号を記憶する空きブロックテーブル等のデータを記憶する。また、SRAM12は、コントローラ15のワークエリアとしても機能し、データを暗号化及び復号化するための暗号化鍵k(復号化されたもの)が一次的に保存される。

【0029】第1のROM(リードオンリメモリ)13は、不揮発性のメモリであり、コントローラ15の動作プログラムを記憶する。第2のROM14は、不揮発性のメモリであり、図2(B)に示すように、暗号化されたデータ鍵kを復号化するための復号プログラムを記憶する復号プログラム記憶エリアT2と、後述する期待値Dを記憶する期待値エリアT3と、ハッシュ関数を記憶するハッシュ関数エリアT4等を備える。

【0030】フラッシュメモリ11, SRAM12, 及

び第1及び第2のROM13、14には、互いに異なった物理アドレスが割り当てられている。また、第2のROM14の、復号プログラムエリアT2、期待値エリアT3、ハッシュ関数エリアT4は、それぞれA1、A2、A3の先頭番地から開始する。

【0031】コントローラ15は、CPU（中央処理装置）、DSP（デジタルシグナルプロセッサ）等から構成され、第1のROM13のプログラムエリアに格納されたプログラムに従って動作し、（1）フラッシュメモリ11へのデータの書き込み動作、（2）フラッシュメモリ11からのデータの読み出し動作、（3）記憶装置10内のメモリをテストするテスト動作を行う。

【0032】コントローラ15は、機能的には、外部のコンピュータ、テスト装置20等にバス（データバス及びコントロールバス）21を介して接続されたI/Oバッファ（インタフェース回路）151と、インタフェース回路151に接続された制御部152と、アドレスカウンタ153と、より構成される。

【0033】アドレスカウンタ153は、内部アドレスバスを介してフラッシュメモリ11、SRAM12、ROM13、14のアドレス端子Addに接続されている。また、制御部152の制御端子は、内部制御バスを介してフラッシュメモリ11、SRAM12、第1及び第2のROM13、14の制御端子Contに接続されている。さらに、制御部152の第1のデータ入出力端子は、データバスを介してフラッシュメモリ11と第1のROM13のデータ端子Dataに接続され、制御部152の第2のデータ入出力端子は、内部データバスを介してSRAM12と第2のROM14のデータ端子Dataに接続されている。

【0034】また、SRAM12、第1のROM13、及びコントローラ15は、樹脂等により一体にモールドされてLSI化されており、SRAM12及び第2のROM14から読み出されたデータがLSIの外部に出力されないように構成されている。

【0035】次に、上記構成の記憶装置10、コンピュータ20及びテスト装置30の動作を説明する。

【0036】（1） 相互認証動作

この記憶装置10を使用する場合、まず、コンピュータ20と記憶装置10の間で相互認証を行う。この相互認証時、コンピュータ20は、例えば、図示せぬ表示画面に「パスワードを入力してください」等のメッセージを表示する。このメッセージに回答して、ユーザがパスワードを入力する。コンピュータ20のドライバとコントローラ15の制御部152は、このパスワードに基づいて、相互に認証し、相互認証に成功すると、記憶装置10の使用を許可して、以後のアクセスを許可する。一方、相互認証に失敗すると、記憶装置10の制御部152は、以後のアクセスを禁止する。

【0037】（2） 書き込み動作

記憶装置10にデータを書き込む場合、コンピュータ20は、バス21を介して記憶装置10に書込コマンドを出力する。この書込コマンドがI/Oバッファ151にセットされる。制御部152は、このコマンドを解釈し、データの書き込みの指示であることを判別すると、図3に示す処理を開始する。まず、制御部152は、I/Oバッファ151を介して、バス21上に書き込みデータの送信を要求するコマンドを出力する（ステップS1）。

【0038】この要求に回答して、コンピュータ20は、書き込みデータの総量と、先頭の論理アドレスを送信する。続いて、コンピュータ20は書き込みデータを順次送信する。

【0039】制御部152は、コンピュータ20から送信されて来たデータ総量と先頭論理アドレスをI/Oバッファ151を介して取り込む（ステップS2）。

【0040】制御部152は、フラッシュメモリ11をアクセスし、暗号化された暗号化鍵kを読み出し、これを第2のROM14の復号プログラムエリアT2に格納された復号プログラムで復号して、平文の暗号化鍵kを生成し、SRAM12に格納する（ステップS3）。この際、第2のROM14から読み出されたデータ（暗号化された暗号化鍵k）及び復号された暗号化鍵kは内部データバスIDを介して転送されるため、LSIの外部からは一切アクセスすることができない。

【0041】次に、制御部152は、フラッシュメモリ11のブート領域T1に格納されているFAT、空きブロックテーブル等を参照し、書き込み対象の空きブロックを特定する（ステップS4）。

【0042】一方、コンピュータ20は書き込み対象のデータをデータバス21上に順次出力する。

【0043】制御部152は、コンピュータ20から供給されるデータを取り込み（ステップS5）、取り込んだデータをSRAM12に保持されている暗号化鍵kを用いて暗号化する（ステップS6）。制御部152は、書き込み制御信号を制御バスCB上に出力し、さらに、データバスDB上に暗号化したデータを出力し、さらに、アドレスカウンタ153に書き込みアドレスを発生させることにより、暗号化されたデータをフラッシュメモリ11に書き込む（ステップS7）。

【0044】制御部152は、あるアドレスについて書き込みが終了すると、全てのデータについて処理を終了したか否かを判別し（ステップS8）、終了していなければ、アドレスカウンタ153を更新して（ステップS9）、ステップS5にリターンして、同様の動作を繰り返す。

【0045】なお、現在の書込対象ブロックが一杯になった場合には、ステップS9で次の空きブロックを選択し、選択した空きブロックのアドレスがアドレスカウンタ153にセットされ、データが次の空きブロックに書

き込まれる。

【0046】制御部153は、データを格納し終わると、フラッシュメモリ11に格納された空きブロックテーブルとFAT及びディレクトリ情報を更新する。さらに、SRAM12に記憶された暗号化鍵kを消去し(ステップS10)、処理を終了する。

【0047】(3) 読み出し動作

記憶装置10からデータを読み出す場合、コンピュータ20は、バス21を介して記憶装置10に読み出しコマンドを出力する。

【0048】読み出しコマンドがI/Oバッファ151にセットされると、制御部152は、このコマンドを解読し、データの読み出しの指示であることを判別し、図4に示す処理を開始する。まず、制御部152は、I/Oバッファ151を介して、バス21上に先頭の論理アドレスと読み出し対象データの総量の送信を要求するコマンドを出力する(ステップS11)。

【0049】この要求に回答し、コンピュータ20は、読み出し対象データの先頭アドレス(論理アドレス)とデータ総量をバス21を介してコントローラ15に通知する。制御部152は、I/Oバッファ151を介して先頭アドレスとデータ総量を受信する(ステップS12)。

【0050】制御部152は、フラッシュメモリ11にアクセスし、暗号化された暗号化鍵kを読み出し、これを第2のROM14の復号プログラムエリアT2に格納された復号プログラムで復号して、平文の暗号化鍵kを生成し、SRAM12に格納する(ステップS13)。この時、第2のROM14から読み出された暗号化された暗号化鍵k及び復号された暗号化鍵kは内部データバスIDBを介して転送されるため、LSIの外部からはアクセスすることができない。

【0051】次に、制御部152は、フラッシュメモリ11に記憶されているFAT及びディレクトリ情報から、読出対象ファイルが格納されている物理アドレスを判別し、アドレスカウンタ153にセットする(ステップS14)。

【0052】次に、制御部152は、読出制御信号を出力し、アドレスカウンタ153が指示する物理アドレスに記憶されたデータを読み出し(ステップS15)、SRAM12に格納した暗号化鍵kを用いて復号化し、復号化したデータをI/Oバッファ151とバス21を介してコンピュータ20に送信する(ステップS16)。

【0053】制御部152は、読み出したデータの総量がコンピュータ20から指示された総量に一致したか否かを判別すること等により、読み出しが終了したか否かを判別する(ステップS17)。読出が終了していない場合には、アドレスカウンタ153は、読出アドレス(物理アドレス)を更新する(ステップS18)。以後、同様にして、物理アドレスを順次更新しながら、デ

ータを読み出す。指定された量のデータを読み終えたと判断されると、コントローラ15は読み出し動作を終了する。

【0054】(4) テスト動作

テスト動作は、通常は、記憶装置10の製造時、出荷時等に行われ、記憶装置10内に配置されているフラッシュメモリ11とSRAM12については、データを正しく記憶し・読み出せるか否か、ROM13, 14については正しいデータが格納されているか否かをテストする。

【0055】このテストモードに設定する場合、記憶装置10は外部のテスト装置30等に接続され、テスト装置30はコントローラ15にテストコマンドを送出する。制御部152は、I/Oバッファ151を介して提供されたテストコマンドに回答し、まず、図5に示すように、フラッシュメモリ11をテストするモードに入る。

【0056】(a) フラッシュメモリ11のテスト

制御部152は、フラッシュメモリ11を一旦初期化する(ステップS21)。続いて、アドレスカウンタ153を制御してアドレスを順次更新しながら、記憶データを順次読み出し、I/Oバッファ151を介してバス21上に出力する(ステップS22)。テスト装置20は、全てのビットが「0」であるか否か、「0」以外のビットが存在する場合には、その物理アドレス等を判別する。

【0057】全てのデータを読み出すと、制御部152は、アドレスを順次更新しながら、全てのビットに値「1」を書き込む(ステップS23)。続いて、アドレスを順次更新しながら、記憶データを読み出し、バス21上に出力する(ステップS24)。テスト装置20は全てのビットが「1」であるか否か、「1」以外のビットが存在する場合には、その物理アドレス等を判別する。

【0058】このようにして、フラッシュメモリ11については、全てのビットをスキャンして、データの書き込み及び読み出しを繰り返すことにより、その良否のチェックが可能となる。

【0059】(b) SRAMのテスト

フラッシュメモリ11のテストが完了すると、制御部152は、SRAM12のテストを開始する。まず、制御部152は、アドレスカウンタ153を制御してアドレスを順次更新しながら、全てのビットに値「1」を書き込む(ステップS25)。続いて、アドレスカウンタ153を制御してアドレスを順次更新しながら、SRAM12の記憶データを読み出し、バス21上に出力する(ステップS26)。テスト装置20は全てのビットが「1」であるか否か、「1」以外のビットが存在する場合には、その物理アドレス等を判別する。

【0060】次に、制御部152は、アドレスを順次更

10

20

30

40

50

新しながら、全てのビットに値「0」を書き込む（ステップS27）。続いて、アドレスを順次更新しながら、SRAM12の記憶データを読み出し、バス21上に出力する（ステップS28）。テスト装置20は全てのビットが「0」であるか否か、「0」以外のビットが存在する場合には、その物理アドレス等を判別する。このようにして、SRAM12についても、全てのビットをスキャンしてチェックが可能となる。

【0061】(c) ROM13、14のテスト
SRAM12のテストが完了すると、制御部152は、ROM13、14のテストを開始する。ROM13、14のテストは、記憶データを読み出し、正しいデータが記憶されているか否かを判別することにより行う。但し、復号プログラムエリアT2の記憶データをそのまま読み出すと、復号プログラムが第三者に知られ、暗号化鍵kが復号されて、盗用又は悪用される虞がある。そこで、暗号化鍵エリアT3については、異なるテスト方法を採用する。

【0062】まず、制御部152は、第1のROM13の先頭アドレスをアドレスカウンタ153にセットする（ステップS29）。次に、制御部152は、アドレスカウンタ153が指示するアドレスが復号プログラムエリアT2のアドレス（ $A1 \leq \text{アドレス} < A2$ ）であるか否かを判別する（ステップS30）。復号プログラムエリアT2のアドレスであると判断された場合、何もせずにアドレスを更新して（ステップS31）、ステップS30にリターンする。

【0063】一方、復号プログラムエリアT2のアドレスではないと判断された場合、そのデータを読み出し（ステップS32）、次のアドレスが存在するか否かを判別し（ステップS33）、存在すれば、アドレスを更新して（ステップS31）、ステップS30にリターンする。このようにして、制御部152は、アドレスカウンタ153を制御してアドレスを順次更新しながら、第1のROM13の記憶データを順次読み出し、I/Oバッファ151を介してバス21上に出力する（ステップS32）。テスト装置30は、第1のROM13から読み出したデータが予め定められた値であるか否かを全データについて判別する。即ち、データが正しく記憶されているか否かを判別する。

【0064】第1のROM13のチェックが完了すると、制御部152は、ステップS31で、第2のROM14の先頭アドレス（A1）をアドレスカウンタ153にセットする。

【0065】次に、制御部152は、アドレスカウンタ153が指示するアドレスが復号プログラムエリアT2のアドレス（ $A1 \leq \text{アドレス} < A2$ ）であるか否かを判別する（ステップS30）。

【0066】復号プログラムエリアT2のアドレスである場合には、アドレスを更新し（ステップS31）、ス

テップS30に戻る。従って、復号プログラムエリアT2については、データは読み出されない。一方、復号プログラムエリアT2のアドレスでない場合には、そのアドレスで指定される位置からデータを読み出し（ステップS32）、バス21上に出力する。続いて、次のアドレスが存在するか否かを判別し（ステップS33）、存在する場合には、ステップS31に戻ってアドレスを更新した後、前述の動作を繰り返す。

【0067】テスト装置30は、提供されるデータが、予め定められている記録パターンと一致するか否か等を判断し、一致しない場合には、そのアドレス等を判別する。

【0068】ステップS33で、次のアドレスが存在しないと判断された場合には、期待値エリアT3及びハッシュ関数エリアT4等のデータの読み出しが終了したので、復号プログラムエリアT2のテストに移る。

【0069】まず、制御部152は、ハッシュ関数エリアT4に記憶されたハッシュ関数Hを読み出す（ステップS34）。次に、期待値エリアT3に格納された期待値のセットDiを読み出す（ステップS35）。制御部152は、ハッシュ関数Hに、復号プログラムエリアT2から順次読み出した所定バイトのデータa、bを代入することにより、 $y_i = H(a, b)$ を求める（ステップS36）。続いて、この値yが、期待値Diに一致するか否かを判別する（ステップS37）。

【0070】制御回路152は、復号プログラムエリアT2の全記憶データを読み出すまで、比較動作を繰り返す。例えば、復号プログラムエリアT2が4kバイトのサイズであり、a、bがそれぞれ512バイトとすれば、4回作業を繰り返す。全ての演算結果と全ての期待値が一致する場合には、一致検出信号をテスト装置20に送信し（ステップS38）、1回でも不一致の場合には、不一致検出信号をテスト装置20に送信する（ステップS39）。以上でテスト動作を終了する。

【0071】このようにして、テスト装置20は、フラッシュメモリ11とSRAM12とに関しては、記憶エリアをスキャンしてデータを記憶させて、さらに、これを読み出して、期待値と比較することにより、テストすることができる。復号プログラムエリアT2を除く第1、第2のROM13、14の記憶エリアに関しても、記憶エリアをスキャンして読み出したデータとプログラム自体とを比較することにより、記憶データの適否を判別できる。

【0072】一方、第2ROM14の復号プログラムエリアT2に関しては、その記憶データを直接読み出すことが、ステップS30で禁止されており、記憶データを直接チェックすることはできず、機密情報である復号化プログラムの漏洩を防止できる。しかも、コントローラ15から供給される比較結果を示すデータから、格納されている復号化プログラムが正しい内容であるか否かを

判別することができる。即ち、演算結果 y と期待値 D が不一致の場合は、何らかの異常が ROM 1 3 内にあると考えられ、そのチップを排除することができる。即ち、このテスト手法によれば、復号化プログラム等の機密情報を第三者であるテスト実施者に公開することなく、記憶装置 1 0 内のメモリの良・不良を検査することができる。

【0 0 7 3】以上説明したメモリテストの機能構成を図 6 に示す。ここに示すように、LSI 内の非プロテクト ROM (外部からアクセスできる ROM)、即ち、第 1 の ROM 1 3 と第 2 の ROM 1 4 の復号プログラムエリアを除く部分は、アドレス指定され、その記憶データが LSI の外部に直接読み出され、外部のチェックパターンと比較される。

【0 0 7 4】一方、LSI 内のプロテクト ROM (外部からアクセスできない ROM)、即ち、第 2 の ROM 1 4 の復号プログラムエリアは、LSI の外部からアドレス指定され、その記憶データを計算モジュールによって変換する。この内容は、RAM に格納され、その RAM の内容から、内部に予め記憶しておいた期待値と比較し、比較結果が外部に出力される。

【0 0 7 5】なお、以上の説明では、プロセッサは、 $D = y (=H(a, b))$ であるか否かを判別することにより、記憶されている暗号鍵の正当性を判別したが、他の手法を使用することも可能である。

【0 0 7 6】例えば、期待値 D を公にしておき、テスト装置 3 0 より、期待値 D を記憶装置 1 0 に提供するようにしてもよい。この場合は、コントローラ 1 5 は、ハッシュ関数エリア T 4 から読み出した関数 $H()$ に暗号化鍵 k を代入して、値を求め、求めた値とコンピュータ本体から提供された期待値 D が一致するか否かを判別し、判別結果をテスト装置 3 0 に供給する。

【0 0 7 7】なお、関数 H は、ハッシュ関数に限定されないが、同一の演算結果に対して複数の変数が対応するものが望ましい。このような構成とすれば、たとえ、期待値 D が第三者に知られても、暗号化鍵 k 自体を特定することはできない。

【0 0 7 8】また、暗号化鍵は、複数でもよい。例えば、第 2 の ROM 1 4 内に全ての記憶装置 1 0 に共通の暗号化鍵 (共通鍵) を記憶させておき、フラッシュメモリ 1 1 にその記憶装置 1 0 に固有の暗号化鍵 (固有鍵) を格納してもよい。この固有鍵は、例えば、記憶装置 1 0 を初期化した際に、乱数等に基づいて設定される。さらに、この固有鍵をパスワード等に基づいて暗号化し、暗号化された固有鍵を復号するためのプログラムをフラッシュメモリに格納してもよい。

【0 0 7 9】また、暗号化の手法として RSA 法を使用する場合には、例えば、公開鍵 e と秘密鍵 n を使用することができる。この場合、暗号化鍵エリア T 3 のテストには、例えば、 $d = m^e \bmod n$ が期待値 D に一致す

るか否かを判別し、判別結果をテスト装置 2 0 に通知するようにしてもよい。この場合、定数 m は外部から供給してもよく、また、予めメモリに格納しておいてもよい。

【0 0 8 0】また、上記説明では、フラッシュメモリ 1 1 及び SRAM 1 2 のチェックのために、「1」及び「0」を全ビットに書き込んだが、例えば、所定のテストパターンを書き込んでも良い。また、さらに、複数回「1」又は「0」を書き込んでも良い。

【0 0 8 1】また、以上の説明では、テスト装置 2 0 からのテストコマンドに回答して、制御部 1 5 2 がアドレスカウンタ 1 5 3 を制御して、アドレスを発生して順次データの書き込み及び読み出しを行ったが、テストモードが設定されると、モードが解除されるまでは、外部のバスと内部バスを直結し、外部 (テスト) からの信号により、直接各メモリをアドレッシングし、且つ、制御信号を出力するように制御してもよい。この場合も、例えば、図 7 に示すように、上位のアドレス信号をデコードする等して、暗号化鍵エリア T 3 がアドレッシングされたときは、ROM 1 3 をディスエイブル状態に設定する等、外部からのアドレッシングを受付けない (禁止する) ように、アドレス信号をマスクすることが望ましい。

【0 0 8 2】(第 2 の実施の形態) 第 1 の実施の形態では、フラッシュメモリ 1 1 にデータを書き込んだり、フラッシュメモリ 1 1 からデータを読み出したたりする間は、SRAM 1 2 に暗号化鍵 k が記憶され、暗号化鍵 k を用いて暗号化及び複合化が行われる。一方、この状態で、動作クロックを停止し、テストモードに入り、SRAM 1 2 の記憶データを読み出すと、暗号化鍵 k が第三者に知られてしまう虞がある。このため、図 8 に示すように、テストモードが指示されると、制御部 1 5 2 が、SRAM 1 2 に一旦リセット信号を送出して、これをリセットし、その後、外部からの制御に従ったテストを可能としてもよい。

【0 0 8 3】以上の説明では、この発明をフラッシュメモリにデータを記憶する際に、データを暗号化及び複合化する暗号化鍵 k を格納する領域のテストに適用した例を説明した。しかし、この発明は上記実施の形態に限定されない。この発明は、機密性を有するデータを記憶した不揮発性記憶媒体のテストに広く適用可能である。

【0 0 8 4】

【発明の効果】以上説明したように、この発明によれば、記憶装置に記憶された機密情報を直接読み出すことなく、機密情報を記憶している領域の良・不良を判別することができる。

【図面の簡単な説明】

【図 1】この発明の実施の形態にかかるメモリ装置及びコンピュータ、さらに、テスト装置の基本構成を示すブロック図である。

15

16

【図 2】ROM の内部構成を示す図である。

【図 3】フラッシュメモリ 11 へのデータ書き込み動作を説明するためのフローチャートである。

【図 4】フラッシュメモリ 11 からのデータの読み出し動作を説明するためのフローチャートである。

【図 5】テスト動作を説明するためのフローチャートである。

【図 6】テスト動作を説明するための機能ブロック図である。

【図 7】機密情報を記憶した領域へのアクセスを禁止する構成の一例を説明するためのブロック図である。

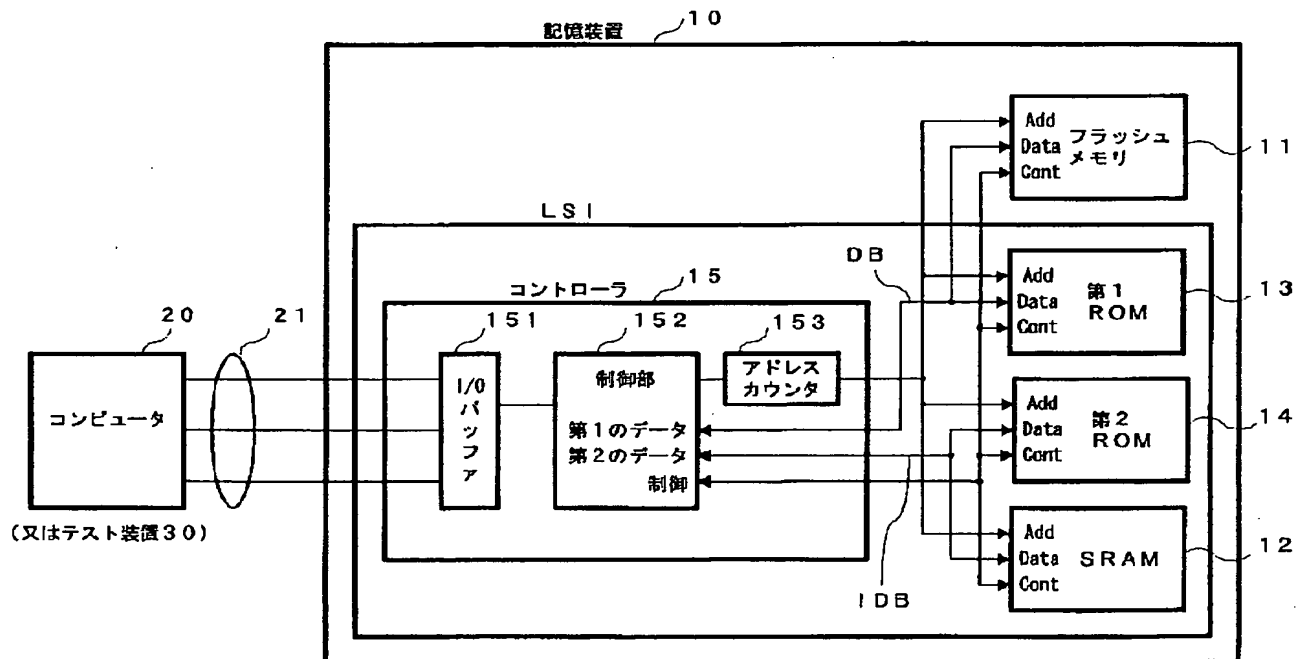
【図 8】テストモードで、SRAM の内容をリセットす

る構成の一例を示す図である。

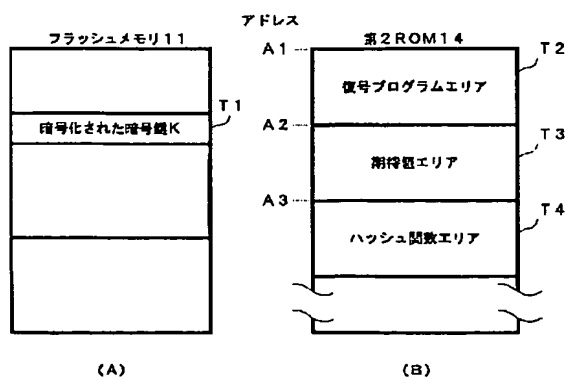
【符号の説明】

11	フラッシュメモリ
12	SRAM
13、14	ROM
15	コントローラ
20	コンピュータ
21	バス
30	テスト装置
151	I/Oバッファ
152	制御部
153	アドレスカウンタ

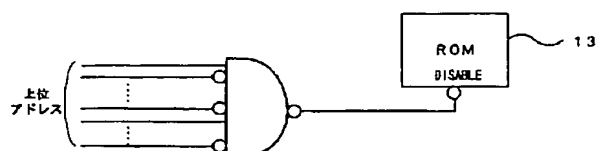
【図 1】



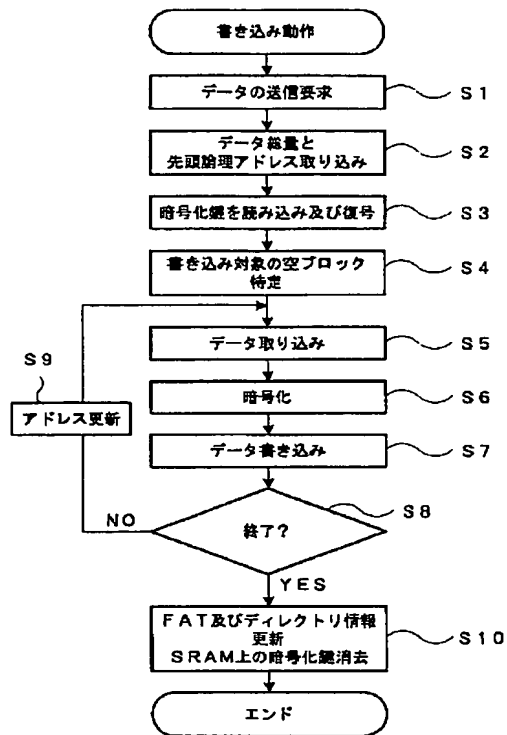
【図 2】



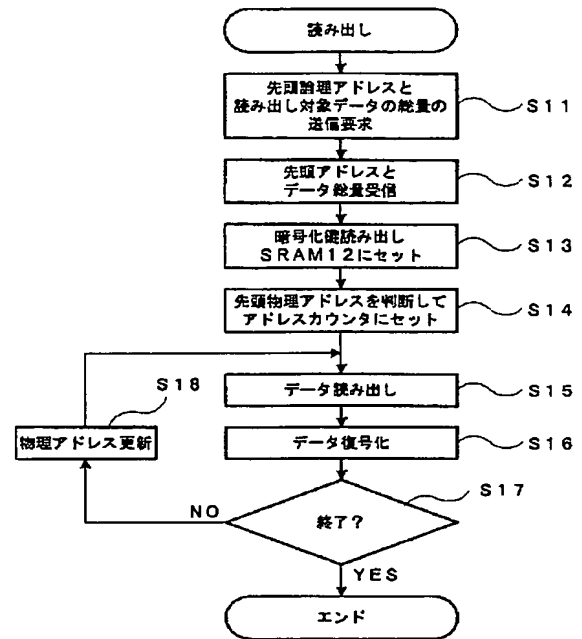
【図 7】



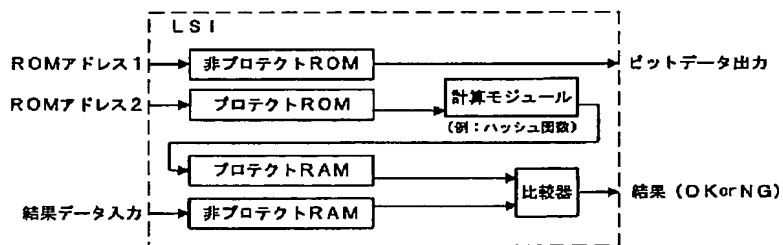
【図3】



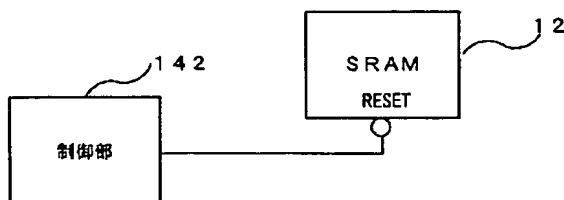
【図4】



【図6】



【図8】



【図5】

